October 18, 2016

Ms. Marlene H. Dortch
Secretary
Federal Communications commission
445 12 Street, SW
Washington, DC 20554

Re: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106

Dear Ms. Dortch:

The Internet Commerce Coalition (ICC) files this Ex Parte letter in the above proceeding in order to report a meeting between Sydney White of DLA Piper LLP (US) on behalf of the Internet Commerce Coalition with Nick Degani, Wireline Advisor to Commissioner Pai, Kirk Arner, Law Clerk to Commissioner Pai, and Amy Bender, Wireline Advisor to Commissioner O'Rielly on October 14, 2016. We focused on the following points: 1) the categories of sensitive information outlined in the Chairman's Fact Sheet are inconsistent with the definition established by the FTC and the White House[1] and do not reflect consumer expectations and 2) the consent requirements for sensitive and non-sensitive data should track the conclusions in the FTC's privacy framework.

Addition of Web Browsing and App Usage as Sensitive Information

During the meeting, we discussed the Protecting the Privacy of Customers of Broadband and Other Telecommunications NPRM and Chairman Wheeler's "Proposal to Give Broadband Consumers Increased Choice Over Their Personal Information". Specifically, Chairman Wheeler's Proposal released on October 6 would have the FCC adopt rules that treat contents of communications, web browsing data and app usage history as equally sensitive data for purposes of the FCC's final broadband privacy rules. If the FCC decides to include contents of communications as part of a category of sensitive information, it should not categorically extend the same level of protection to "non-content" web browsing information and app usage history as

[1]Sensitive data categories have been defined in FTC guidance and the White House 2012 Privacy Report as health information, children's information, financial account data and SSNs and the same categories plus communications contents should apply in the final order.

these elements do not necessarily merit additional protections. Additionally, IP addresses should not in all instances be characterized as personal information, as was suggested in the NPRM as long as they are not combined with identifiable data.

We discussed how a core feature of the privacy framework of the Obama Administration and the FTC has been technology-neutral requirements that provide strong, consistent privacy protections for consumers. This approach benefits consumers because it avoids confusing consumers about the extent to which their privacy is protected online through obscure variations in privacy rules based upon the type of business of the entities with which consumers conduct business online. A consistent approach of the sort that the FTC Comments proposed would also avoid a First Amendment challenge based upon the rules providing a different approach for Internet advertising.

We discussed that the FTC Comments did not suggest that non-content web browsing or app usage information should be subject to an opt-in consent requirement, and because this requirement is not consistent with FTC precedent, including this requirement in the final order would create a very different rule for ISPs than the regime that applies for the rest of the Internet ecosystem.

The FTC has examined the question of what qualifies as content, and it is well-established that neither URL addresses of Internet sites visited by a consumer, much less app usage data, are necessarily sensitive information that would require an opt-in consent. And the FTC has determined that implied consent or opt-out choice is appropriate for the use of all non-sensitive web browsing history, and this is the approach that applies throughout the Internet ecosystem today.

We discussed that Section 222 of the Communications Act does not reflect a Congressional judgment that all information handled by telecommunications carriers is sensitive. For example, Section 222 has an exception for "subscriber list information" which is not subject to the same protections as CPNI and which carriers are required to make publically available for competitive reasons.

Operationalizing a Sensitivity Based Approach

We discussed that Internet companies, including ISPs, routinely implemented protections so as to not target advertising or market to consumers on the basis of sensitive data categories, unless opt-in consent is obtained.[2] This distinction is a key part of the Digital Advertising Alliance and Network Advertising Initiative self-regulatory frameworks, in which many Internet companies, including ISPs, participate. The participants are subject to enforcement, by

[2] For additional background on operationalizing a sensitivity based approach, see Internet Commerce Coalition Ex Parte Notice also filed on 10/18/16 for the 10/14/16 meeting between Jim Halpert and Sydney White of DLA Piper LLP (US) with Gigi Sohn, Counselor to Chairman Wheeler, Matt DelNero Bureau Chief Wireline Competition Bureau, Lisa Hone, Associate Bureau Chief Wireline Competition Bureau, and Stephanie Weiner, Wireline Advisor to Chairman Wheeler.

government regulators and industry regulatory bodies, and the FCC would have even stronger enforcement levers to ensure compliance.

We discussed the argument made by some consumer advocates that ISPs must intrusively scan the content of customers' communications to avoid using sensitive personal information for advertising. To the contrary, ISPs and other Internet companies avoid the use of sensitive personal information for advertising by categorizing website URLs and app usage based on standard industry interest categories. ISPs and other Internet companies "black list" and wall off web browsing and other data from sites that fall into sensitive categories and therefore avoid using these specific types of content as inputs for advertising programs without user consent. Companies in the Internet advertising ecosystem routinely manage these lists as a way to avoid using web browsing history or other data in a way that raises sensitivity concerns.

It is incorrect to assume that ISPs must intrusively scan the content of customers' web browsing to avoid using sensitive data for advertising and marketing purposes. In fact, it is relatively straightforward for ISPs to categorically exclude, for example, health or financial information for advertising via coding instructions that allow ads to be served based only upon data from white listed sources and/or through algorithms and other coding techniques that exclude data associated with sensitive categories of information.

For this reason, there is no operational compliance barrier that justifies departing from the FTC's recommended approach: to limit the scope of the opt-in requirement to the specific sensitive information categories identified in the FTC and White House privacy frameworks plus contents of communications. This would apply to a subset of web browsing and app usage information that is actually sensitive, and could be adjusted in the future if deemed necessary. However, the FCC should reject proposals to categorize all web browsing and app usage as sensitive information, as they are clearly not treated as such under the FTC, White House and ECPA privacy frameworks.

Conclusion

The final FCC rules should reserve opt-in consent for the elements of sensitive data identified by the FTC Comments, consistent with FTC precedent, and should otherwise apply the opt-out or implied consent approach set forth in the FTC's 2012 Privacy Report. For example, first-party marketing of an ISP's other products and services should be permissible based on implied consent, as both the FTC and Administration have previously concluded.

Respectfully submitted,

/s/ **Sydney M. White**

Jim Halpert
Sydney M. White
Counsel to Internet Commerce Coalition